**DETAILED ACTION**

***Examiner's Amendment***

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's Amendment was given in a telephone interview with Kevin M. Mason (Reg. No. 36,597) on 16 April 2009.

This application has been amended as follows:

IN THE CLAIMS

**Cancel claim 2, 3, 7 and 14.**

**Replace claim 1, 4 – 6, 8, 10, 11 and 13 as follows.**

**Claim 1**

A method for compressing a Rabin signature, s, for a user having a public key, n, comprising ~~the step of~~:

configuring a processor to perform the steps of:

compressing said ~~generating a compressed~~ Rabin signature using ~~based on~~ a continued fraction expansion of s/n, wherein said continued fraction expansion of s/n further comprises the steps of :

computing principal convergents, $u_i/v_i$, for i equal to 1 to k, of a continued fraction expansion of s/n, where k is a largest integer for which principal convergents are defined, where $u_i$ and $v_i$ are principal convergents, and where a greatest common denominator (s, n) ≠ 1;

establishing an index *l*, such that $v_l < \sqrt{n} < v_{l+1}$; and generating a compressed Rabin signature ($v_l$, m) for a message, m, using said continued fraction expansion of s/n.

**Claim 4**

The method according to claim 1 ~~3~~, wherein sv=u (mod n).

**Claim 5**

The method according to claim 1 ~~3~~, wherein $|v| \leq \sqrt{n}$.

**Claim 6**

The method according to claim 1 ~~3~~, wherein $|u| \leq \sqrt{n}$.

**Claim 8** A method for decompressing a compressed Rabin signature (v, m) for a message, m, and user having a public key, n, comprising ~~the steps of~~:

configuring a processor to perform the steps of:

applying a message formatting function, h, to the message, m, to computing h(m);

computing a value, t, as $h(m)v^2$ mod n;

obtaining a value, w, as a square root of the value, t;

computing a signature value, s, as w/v mod n; and

providing a decompressed signature (s,m).

**Claim 10**

A method for compressing an RSA signature, s, for a message, m, and a user having a public key (n, e), comprising ~~the steps of~~:

configuring a processor to perform the steps of:

computing principal convergents, $u_i/v_i$, of for i equal to 1 to k, a ~~the~~ continued fraction expansion of s/n, where k is a largest integer for which principal convergents are defined, where $u_i$ and $v_i$ are principal convergents, and where a greatest common denominator (s, n) ≠ 1;

establishing an index I, such that $v_i < n^{(1-1/e)} \leq v_{i+1}$; and

generating a compressed RSA signature ($v_i$, m) using said continued fraction expansion of s/n.

**Claim 11**

A method for decompressing a RSA signature (v, m) for a message, m, and a user having a public key (n, e), comprising ~~the steps of~~:

configuring a processor to perform the steps of:

applying a message formatting function, h, to the message, m, to computing h(m);

computing a value, t, as $h(m)v^e$ mod n;

determining whether the values t or t-n have an $e^{th}$ root over integer values;

computing a value, w, as the $e^{th}$ root; and computing the decompressed signature (w/v mod n, m).

**Claim 13**

A system for compressing a Rabin signature, s, for a user having a public key, n, comprising:

a memory; and

at least one processor, coupled to the memory, operative to:

compress said ~~generate a compressed~~ Rabin signature using ~~based on~~ a continued fraction expansion of s/n, wherein said processor is further configured to perform said continued fraction expansion of s/n by:

computing principal convergents, $u_i/v_i$, for i equal to 1 to k, of a continued fraction expansion of s/n, where k is a largest integer for which principal convergents are defined, where $u_i$ and $v_i$ are principal convergents, and where a greatest common denominator (s, n) ≠ 1;

establishing an index *l*, such that $v_l < \sqrt{n} < v_{l+1}$; and

generating a compressed Rabin signature ($v_l$, m) for a message, m, using said continued fraction expansion of s/n.

***Allowable Subject Matter***

Claims 1, 4 – 6, 8 – 13, 15 and 16 are allowed.

The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations recited in claims 1, 8, 10, 11, 13 and 15 (& associated dependent claims) and the claims 1, 4 – 6, 8 – 13, 15 and 16 are allowable in light of the Applicant's arguments and in light of the prior art made of record.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Primary Patent Examiner
Art Unit 2431
4/02/2009